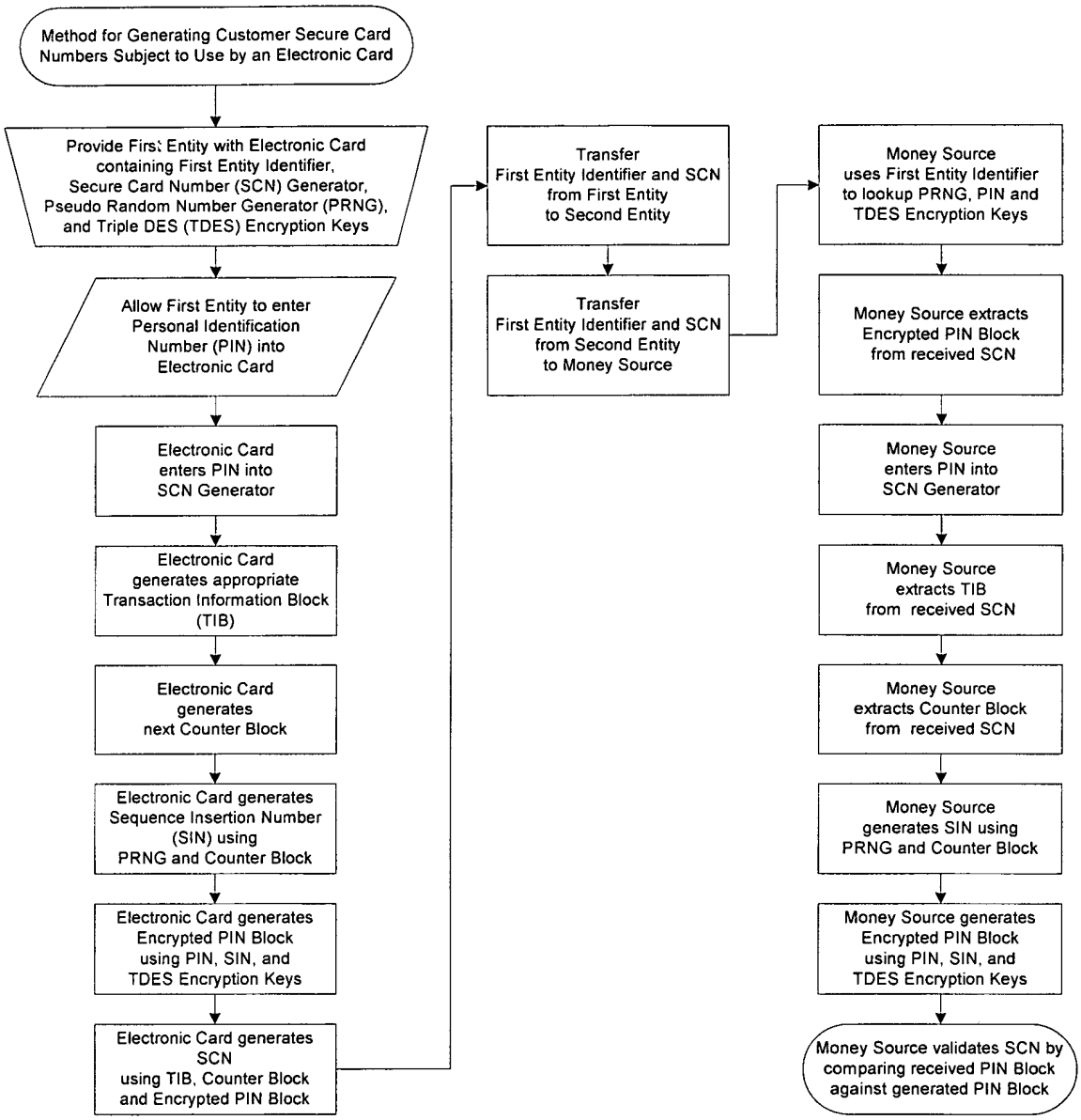
Figure 1


Method for Generating Customer Secure Card Numbers Subject to Use by an Electronic Card
Provide First Entity with Electronic Card containing First Entity Identifier, Secure Card Number (SCN) Generator, Pseudo Random Number Generator (PRNG), and Triple DES (TDES) Encryption Keys
Allow First Entity to enter Personal Identification Number (PIN) into Electronic Card
Electronic Card enters PIN into SCN Generator
Electronic Card generates appropriate Transaction Information Block (TIB)
Electronic Card generates next Counter Block
Electronic Card generates Sequence Insertion Number (SIN) using PRNG and Counter Block
Electronic Card generates Encrypted PIN Block using PIN, SIN, and TDES Encryption Keys
Electronic Card generates SCN using TIB, Counter Block and Encrypted PIN Block
Transfer First Entity Identifier and SCN from First Entity to Second Entity
Transfer First Entity Identifier and SCN from Second Entity to Money Source
Money Source uses First Entity Identifier to lookup PRNG, PIN and TDES Encryption Keys
Money Source extracts Encrypted PIN Block from received SCN
Money Source enters PIN into SCN Generator
Money Source extracts TIB from received SCN
Money Source extracts Counter Block from received SCN
Money Source generates SIN using PRNG and Counter Block
Money Source generates Encrypted PIN Block using PIN, SIN, and TDES Encryption Keys
Money Source validates SCN by comparing received PIN Block against generated PIN Block